CLAIMS

What is claimed is:

1. A method of performing encryption key management in an AC powerline communication network system, wherein the communication network system includes at least one receiving client device and at least one originating client device, and wherein the at least one receiving client device lacks user input capability, and wherein the at least one originating client device has user input capability, comprising the steps of:

   (a) inputting one of a hard-wired key and a password into the at least one originating client device;

   (b) creating an encryption key update payload message comprising a current network encryption key encrypted by a hard-wired key;

   (c) transmitting the encryption key update payload message from the at least one originating client device to the at least one receiving client device; and

   (d) replacing a previous network encryption key with the current network encryption key in the at least one receiving client device.

2. The method of performing encryption key management as set forth in Claim 1, further comprising the steps of:

   (e) creating a key update acknowledgement payload message comprising the hard-wired key encrypted by the current network encryption key;

   (f) transmitting the key update acknowledgement payload message from the at least one receiving client device to the at least one originating client device; and

   (g) re-transmitting the encryption key update payload message transmitted in sub-step (c) of Claim 1 until the at least one originating client device receives the key update acknowledgment payload message from the at least one receiving client device, then terminating.

3. The method of performing encryption key management as set forth in Claim 1, wherein the inputting step (a) comprises the sub-steps of:

(1) selecting an encryption key algorithm; and

(2) inputting one of a hard-wired key and a password into the at least one originating client device.

4. The method of performing encryption key management of Claim 3, wherein the encryption key algorithm is a Data Encryption Standard.

5. The method of performing encryption key management of Claim 4, wherein the Data Encryption Standard operates as a stream cipher in output feedback mode.

6. The method of performing encryption key management of Claim 5, wherein a keystream is applied only to payload bits.

7. The method of performing encryption key management of Claim 3, wherein a client device indicates supported encryption algorithms using beacon payload messages.

8. The method of performing encryption key management of Claim 1, wherein the encryption key update payload message includes a payload, and wherein the payload includes an initialization vector and a forward error correction.

9. The method of performing encryption key management of Claim 8, wherein the payload includes a logical network identifier currently in use in the logical network.

10. The method of performing encryption key management of Claim 8, wherein the forward error correction comprises a 32-bit cyclic redundancy code (CRC).

11. The method of performing encryption key management of Claim 1, wherein the creating step (b) comprises the sub-steps of:

(1) computing a CRC over an entire encryption key update payload; and

(2) encrypting a key field and a CRC field.

12. The method of performing encryption key management of Claim 2, wherein the creating a key update acknowledgment step (e) comprises the sub-steps of:

(1) selecting a new initialization vector;

(2) filling an encryption key field with the hard-wired key;

(3) computing a CRC over an entire key update acknowledgment payload; and

(4) encrypting the encryption key field and a CRC field.

13. The method of performing encryption key management of Claim 2, wherein the re-transmitting step (g) comprises the sub-steps of:

(1) awaiting receipt of a beacon payload message from the at least one receiving device; and

(2) re-transmitting the encryption key update payload message transmitted in sub-step (c) of Claim 1 until the at least one originating client device receives the key update acknowledgment payload message, then terminating.

14. An encryption key management AC powerline networking circuit, comprising:

(a) at least one originating client device, capable of receiving user input, adapted to input a hard-wired key and a password, wherein the originating client device is adapted to create an encryption key update payload message comprising a current network encryption key encrypted by the hard-wired key, and wherein the originating client device is adapted to transmit the encryption key update payload message to another client device; and

(b) at least one receiving client device, operatively coupled to the at least one originating client device, wherein the receiving client device is adapted to receive the encryption key update payload message, and adapted to create a key update acknowledgment payload message comprising the hard-wired key encrypted by a current network encryption key.

15. The circuit of Claim 14, wherein the receiving client device is incapable of receiving user input.

16. An AC powerline networking circuit for managing encryption keys, comprising:

(a) means for inputting one of a hard-wired key and a password;

(b) means, responsive to the input means, for encrypting a current network encryption key utilizing a hard-wired key and for encrypting the hard-wired key utilizing a current network encryption key;

(c) means, operatively coupled to the encrypting means, for transmitting an encryption key update payload message to a first device and for transmitting a key update acknowledgment payload message to a second device; and

(d) means, responsive to the transmitting means, for receiving a beacon, the encryption key update payload message and the key update acknowledgment payload message.

17. The circuit of Claim 16, wherein the first device is incapable of receiving user input.

18. An AC powerline networking circuit for managing encryption keys, comprising:

(a) means for inputting one of a hard-wired key and a password to a first device;

(b) a first encrypting means, responsive to the input means, for encrypting a current network encryption key utilizing a hard-wired key;

(c) a first transmitting means, operatively coupled to the first encrypting means, for transmitting an encryption key update payload message to a second device;

(d) a first receiving means, operatively coupled to the first transmitting means, for receiving the encryption key update payload message;

(e) means, operatively coupled to the first receiving means, for decrypting the encryption key update payload message;

(f) a second encrypting means, operatively coupled to the decrypting means, for encrypting the hard-wired key utilizing the current network encryption key;

(g) a second transmitting means, operatively coupled to the second encrypting means, for transmitting a key update acknowledgment payload message to the first device; and

(h) a second receiving means, operatively coupled to the second transmitting means, for determining if a beacon and the key update acknowledgment payload message is received by the first device.

19. The circuit of Claim 18, wherein the second device is incapable of receiving user input.

20. A method of managing multiple MAC protocols in an AC powerline communication network system, wherein the communication network system comprises a plurality of devices, and wherein a first set of the plurality of devices uses a first MAC protocol and wherein a second set of the plurality of devices uses a second MAC protocol, and wherein the first MAC protocol is a previous MAC version and the second MAC protocol is a current MAC version, comprising the steps of:

(a) selecting a newer-version MAC protocol device to control a blanking interval;

(b) determining a period and a duration of the blanking interval of step (a);

(c) transmitting a message at a predetermined interval, wherein the message specifies the period and the duration of the blanking interval;

(d) allowing devices using the second MAC protocol to perform contention-based access during the blanking interval; and

(e) allowing devices using the first MAC protocol to perform contention-based access during a special contention resolution slot.

21. The method of managing multiple MAC protocols of Claim 20, wherein the current MAC version is a non-v1.0 MAC version and the previous version is a v1.0 MAC version.

22. The method of managing multiple MAC protocols of Claim 20, wherein the predetermined interval is approximately five seconds.

23. The method of managing multiple MAC protocols of Claim 20, wherein the determining step (b) comprises the sub-steps of:

(1) monitoring communication traffic; and

(2) determining a period and a duration for the blanking interval based upon the communication traffic monitored during sub-step (1).

24. The method of managing multiple MAC protocols of Claim 20, wherein the message is a medium blanking payload message, and wherein the medium blanking payload message specifies the period and the duration.

25. The method of managing multiple MAC protocols in an AC powerline communication network system of Claim 20, wherein the message comprises a medium blanking payload message and a beacon message, and wherein the beacon message specifies the period and the duration.

26. The method of managing multiple MAC protocols in an AC powerline communication network system of Claim 20, wherein the transmitting step (c) comprises transmitting a ROBO-mode broadcast packet including a medium blanking payload message, wherein the medium blanking payload message specifies the period and the duration.

27. The method of managing multiple MAC protocols in an AC powerline communication network system of Claim 20, wherein the message transmitted at the step (c) provides a network timing reference and network timing information pertaining to the blanking interval.

28. The method of managing multiple MAC protocols in an AC powerline communication network system of Claim 20, wherein the method further includes a random backoff step wherein devices having queued packets for transmission randomly transmit their queued packets after the blanking interval.

29. The method of managing multiple MAC protocols in an AC powerline communication network system of Claim 20, wherein the method further includes a random backoff step wherein devices having queued packets for transmission transmit their queued packets immediately subsequent to the blanking interval.

30. A method of controller-less reservation based access in an AC powerline communication network system, wherein the communication network system includes a plurality of communication clients, comprising the steps of:

(a) broadcasting a reservation establishment payload that establishes a reservation between an originating client and a recipient client;

(b) determining a reservation schedule based upon clients that have active reservations, wherein the reservation schedule includes a plurality of reservation access periods, and wherein a specified originating client and a specified recipient client communicate during a specified reservation access period;

(c) transmitting information between clients during the plurality of reservation access periods based upon the reservation schedule determined during step (b); and

(d) determining whether to renew or to terminate reservations.

31. The method of controller-less reservation based access of Claim 30, wherein the step (a) of broadcasting a reservation establishment payload comprises broadcasting a ROBO mode packet comprising a reservation establishment payload.

32. The method of controller-less reservation based access of Claim 30, wherein the reservation establishment payload includes information pertaining to reservation start time, packet duration, transmission period and reservation lifetime.

33. The method of controller-less reservation based access of Claim 30, wherein the reservation includes a two-way reservation, and wherein the two-way reservation comprises a forward transmission and a reverse transmission.

34. The method of controller-less reservation based access of Claim 30, wherein the broadcasting step (a) comprises the sub-steps of:

(1) broadcasting a ROBO mode packet including a reservation establishment payload; and

(2) transmitting a reservation acknowledgement payload from the recipient client.

35. The method of controller-less reservation based access of Claim 33, wherein the forward transmission and the reverse transmission have the same transmission period.

36. The method of controller-less reservation based access of Claim 30, wherein the reservation comprises a one-way reservation, and wherein the one-way reservation comprises a forward transmission.

37. The method of controller-less reservation based access of Claim 30, wherein reservations are renewed by broadcasting a ROBO mode packet including a reservation renewal payload message.

38. The method of controller-less reservation based access of Claim 30, wherein reservations are renewed and terminated only after the occurrence of a last reservation access period.

39. The method of controller-less reservation based access of Claim 30, wherein reservations are renewed and terminated only immediately subsequent to the occurrence of a last reservation access period.

40. The method of controller-less reservation based access of Claim 30, wherein reservations are terminated in accordance with the following sub-steps:

(1) loading a zero value into a reservation lifetime field in a reservation renewal payload message; and

(2) transmitting the reservation renewal payload message.

41. A method of identifying logical networks in an AC powerline communication network system, wherein the communication network system comprises a plurality of communication clients, and wherein each client is uniquely associated with a logical network, the method comprising the steps of:

(a) determining a unique logical network identifier (LNI) for a selected plurality of clients;

(b) broadcasting information regarding the unique LNI;

(c) creating tables that map client addresses to the LNI; and

(d) communicating data only between the selected plurality of clients associated with the unique LNI.

42. The method of identifying logical networks in an AC powerline communication network system of Claim 41, wherein the determining step (a) comprises the sub-steps of:

(1) inputting a password; and

(2) hashing the password to map the password to a logical network identifier (LNI).

43. The method of identifying logical networks in an AC powerline communication network system of Claim 42, wherein the hashing sub-step (2) comprises compressing the password into a 32-bit LNI by generating a 32-bit CRC code for the password.

44. The method of identifying logical networks in an AC powerline communication network system of Claim 42, wherein the password comprises a street address of an owner of the AC powerline communication network.

45. The method of identifying logical networks in an AC powerline communication network system of Claim 42, wherein the password comprises a network name.

46. The method of identifying logical networks in an AC powerline communication network system of Claim 42, wherein the password is input during installation of the AC powerline communication network.

47. The method of identifying logical networks in an AC powerline communication network system of Claim 41, wherein the LNI is communicated to the selected plurality of clients via a beacon payload message.

48. The method of identifying logical networks in an AC powerline communication network system of Claim 43, wherein the 32-bit CRC code for the password is formed by using an ASCII-mapped translation of the password in accordance with the following CRC polynomial:

$$g(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x^1 + 1.$$

49. The method of identifying logical networks in an AC powerline communication network system of Claim 43, wherein the LNI has a selected length of N bits, and wherein the LNI is obtained by generating an N-bit CRC code for the password.

50. A method of controlling communication between devices in an AC powerline communication network system, wherein a first set of the devices uses a first MAC protocol and wherein a second set of the devices uses a second MAC protocol, wherein the first MAC protocol is a previous MAC version and the second MAC protocol is a current MAC version, and wherein medium blanking messages are transmitted on the network by a controlling one of the second set of devices, wherein the blanking messages contain blanking information that defines a blanking interval during which only the second set of devices are allowed to communicate, comprising the steps of:

(a) determining whether a selected device is capable of receiving the blanking messages from the controlling device;

(b) if the selected device is capable of receiving the blanking messages, assembling a respective and associated beacon message unique to the selected device, wherein the assembled beacon message is based upon information contained in received blanking messages, and wherein the beacon message includes blanking information contained in the received blanking messages, and proceeding to step (d), else proceeding to step (c);

(c) if the selected device is incapable of receiving the blanking messages, assembling the beacon message based upon beacon messages received from other network devices, wherein each beacon message includes a lifetime field that is used by all of the devices in determining whether to use a received beacon message when assembling their respective and associated beacon messages; and

(d) periodically transmitting the beacon message assembled in steps (b) or (c) to other devices in the network.

51. The method of controlling communication between devices in an AC powerline communication network system of Claim 50, wherein the current MAC version is a non-v1.0 MAC version and the previous MAC version is a v1.0 MAC version.

52. The method of controlling communication between devices in an AC powerline communication network system of Claim 50, wherein the lifetime field of the assembled beacon message is set to zero whenever the selected device receives a blanking message from the controlling device.

53. The method of controlling communication between devices in an AC powerline communication network system of Claim 50, wherein the lifetime field of the assembled beacon message is set to a non-zero number whenever the selected device is incapable of receiving blanking messages from the controlling device.

54. The method of controlling communication between devices in an AC powerline communication network system of Claim 50, wherein the selected device is determined incapable of receiving blanking messages only if it has not received a blanking message within a predetermined threshold of time.

55. The method of controlling communication between devices in an AC powerline communication network system of Claim 54, wherein the predetermined threshold comprises 5 seconds.

56. The method of controlling communication between devices in an AC powerline communication network system of Claim 53, wherein the non-zero number comprises a lowest lifetime field value of all beacon messages received by the selected device within a predetermined recent time period.

57. The method of controlling communication between devices in an AC powerline communication network system of Claim 56, wherein the recent time period comprises the most recent 5 seconds.

58. The method of controlling communication between devices in an AC powerline communication network system of Claim 50, wherein when the selected device is incapable of receiving blanking messages, the selected device assembles its respective and associated beacon message based upon a received basis beacon message, wherein the basis beacon message comprises a received beacon message having a lowest lifetime field value of all received beacon messages.

59. The method of controlling communication between devices in an AC powerline communication network system of Claim 58, wherein only beacon messages received within a recent time period are considered in determining the basis beacon message.

60. The method of controlling communication between devices in an AC powerline communication network system of Claim 59, wherein the recent time period comprises the most recent 5 seconds.

61. The method of controlling communication between devices in an AC powerline communication network system of Claim 59, wherein when two or more received beacon messages have equally low lifetime field values, the basis beacon message comprises a most recently received beacon message having the equally low lifetime field value.

62. The method of controlling communication between devices in an AC powerline communication network system of Claim 59, wherein the selected device sets a lifetime field value of its assembled beacon message equal to the lifetime field value of the basis beacon message, incremented by one.

63. The method of controlling communication between devices in an AC powerline communication network system of Claim 50, wherein the lifetime field value of all beacon messages has a predetermined maximum.

64. The method of controlling communication between devices in an AC powerline communication network system of Claim 63, wherein the predetermined maximum is 7.

65. The method of controlling communication between devices in an AC powerline communication network system of Claim 63, wherein when all of the beacon messages transmitted on the network have lifetime field values equal to the maximum, the blanking interval is assumed to be nonexistent, and the devices are allowed to transmit at any time.

66. The method of controlling communication between devices in an AC powerline communication network system of Claim 50, wherein the beacon messages are used to specify a period and duration of the blanking interval, and an exact time instant at which the blanking interval begins.

67. The method of controlling communication between devices in an AC powerline communication network system of Claim 50, wherein the beacons contain information regarding the capability and limitation of the devices in the network.